Health Care Authority

Administrative Policy No. 1-13

Chapter 1: Agency Administration

Contact:	HCA Audit Manager Information Services Manager	Effective:	
		Issued:	
Reference:	RCW 42.52.160 WAC 292-110-010 HCA Policy 1-04, Using State Resources	Supersedes:	1-13, Computer Use (6/13/2000)
Forms Used:	Information Technology Use Acknowledgement Form IT Use Acknowledgement Form	Approved by:	Administrator

Using Information Technology Assets

PURPOSE

This policy explains the guidelines for use of information technology (IT) assets within the agency on HCA-provided computer hardware and software. It applies to both on-site and off-site IT asset use when performing official HCA business.

DEFINITIONS

IT Assets

IT assets include, but are not limited to: mainframes, personal computers, personal digital assistants and laptops; software and other related equipment; and communications media that generate, store, transmit, and display correspondence provided for internal and external HCA business communication purposes (e.g., telephones, FAX machines, printers, scanners, voicemail, Internet, electronic mail, etc.) owned or leased by the HCA, Department of Information Services (DIS), or other state agencies.

Employee

Any HCA employee, consultant, contractor, or temporary service employee doing business on behalf of the HCA.

POLICY

1. **All employees shall read this policy and complete and sign the *Information Technology Use Acknowledgement Form* (HCA 40-205).**

   a. By signing the form, employees acknowledge that they have read this policy.

   b. A copy of the form shall be forwarded to the HCA Help Desk and the original forwarded to Human Resources.

APPROVED
Executive Ethics Board
Date: 6/6/03

2. **Employees shall use the HCA-provided IT systems and software for official use only, except as allowed for within this policy.**

3. **This policy applies to the usage of all HCA-provided IT assets.**

   a. This includes usage during break periods, lunch periods, any and all other "non-duty" periods, and use of HCA-provided IT systems while off the HCA premises.

   b. All IT assets and data stored within are considered state property.

4. **All messages composed, sent, or received on HCA IT assets are and remain the property of the HCA.**

   a. Messages may be monitored and reviewed within the agency and also may be considered publicly discoverable in a court of law.

   b. The confidentiality of any message should not be assumed. Even when a message is erased or deleted, it may still be possible to retrieve and read that message.

5. **Employees shall not use state-provided IT assets for the creation and distribution of any offensive or disruptive messages, copyright infringement, or any other unlawful activity.**

   This may include:

   a. Any use for the purpose of personal benefit such as conducting an outside business or private employment (examples include a commercial contest or searching for jobs other than employment sponsored by the Dept. of Personnel).

   b. Any use for the purpose of supporting, promoting the interests of, or soliciting for an outside organization or group including, but not limited to: a private business, a non-profit organization or a political party (unless provided by law or authorized by an agency head).

   c. Disseminating or printing of copyrighted materials, including articles and software, in a manner that violates copyright laws.

   d. Sending or printing offensive or harassing statements or language. Messages that may be construed as offensive contain sexual innuendoes, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, creed, color, religious or political beliefs, national origin, or disability.

   e. Sending or soliciting sexually oriented messages or images.

   f. Promoting or supporting any religious or political causes or non-agency business-related events.

   g. Sending or printing chain letters.

   h. Gambling or engaging in any other activity in violation of local, state, or federal laws.

APPROVED
Executive Ethics Board
Date: 6/6/03

i. Viewing or disseminating statements that might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.

j. Attempting to access another user's files or e-mail messages without the user's knowledge. Special unique circumstances will be coordinated with the HCA's Audit Manager.

k. Gaining or attempting to gain access to protected agency resources.

l. Participating in non-business related chat groups, list servers, or news groups.

m. Operating, advertising, or promoting a non-agency endorsed event.

n. Forge or attempt to forge email messages, or disguise or attempt to disguise your identity when sending email or any other type of correspondence.

The above examples are not all-inclusive. HCA employees have historically shown good judgment in the appropriate use of HCA resources; IT assets are merely another form of WA State resources. Employees are encouraged to ask themselves whether a particular computer access or operation would be considered "work related" and appropriate by their supervisor. As in virtually every instance like this, common sense is often a very effective guide.

6. De Minimis Personal use of the Internet and electronic mail will be allowed, except as noted under section 5 above.

a. De minimis use means that the use meets all of the following tests:

i. There is little or no cost to the state.

ii. Any use if brief, occurs infrequently, and is the most effective use of time or resources.

iii. The use does not interfere with the performance of the officer or employee's official duties.

iv. The use does not disrupt or distract from the conduct of state business due to volume or frequency.

v. The use does not disrupt other state employees and does not obligate them to make a personal use of state resources. (Examples to avoid include mass personal emails and chain letters.)

vi. The use does not compromise the security or integrity of state property, information, or software.

b. De minimis use of agency technology resources does not include services that use excessive agency bandwidth such as large file downloading or sending out large files unless authorized for business purposes (examples include viewing video or listening to Internet radio broadcasts.)

c. Some examples of the types of activities that currently are allowed on a de minimis basis (as long as the de minimis use criteria listed above are met) are:

APPROVED
Executive Ethics Board
Date: 6/6/03

i. To check on your children or childcare arrangements via E-mail.
ii. To notify HCA employees of Administrator approved charitable activities.
iii. To notify HCA employees of retirement events.
iv. To check on personal Deferred Compensation account activity.
v. To check on personal medical insurance information on the HCA website.

7. **No IT assets may be purchased, removed, or discarded without prior coordination with Information Services (I.S.).**

a. Emerging IT asset requirements, especially computer and software needs, shall be identified to I.S. via a Service Request.

b. I.S. will then work with the requesting division/section to conduct a requirements analysis, making sure that the equipment is compatible with the HCA's current infrastructure.

c. I.S. will then coordinate with the division/section requiring the hardware/software and Administrative Services to have the appropriate hardware/software purchased.

8. **Users must not disconnect or move IT assets without first coordinating with I.S.**

9. **Lost, stolen, or damaged IT assets must be reported immediately to the Administrative Services Manager.**

10. **The Information Services Manager, in coordination with the Audit Manager, is responsible for recommending and enforcing agencywide standards necessary to ensure IT asset security.**

The following steps will be taken to provide a secure computing environment:

a. Each employee is responsible for protecting the confidentiality of his/her passwords. If a user must record his/her passwords, that information must be stored in a secure manner such as in a sealed envelope in a locked drawer or container.

b. Users must not embed user IDs and/or user ID passwords into any macro.

c. Individual system log-on passwords must not be shared. In the event a supervisor needs to gain access to or information regarding a user's account, files or emails (i.e., the user is on leave and an essential document is located in the employee's home directory), the supervisor shall first coordinate with the Audit Manager. The Audit Manager will then contact I.S. to change the employee's log-on password to enable the supervisor to access the needed files. Immediately after the necessary information is retrieved, I.S. will change the user's password again and ensure the system prompts the user to change that password as soon as the next log-on occurs.

d. If a user password protects a file, the file name and password shall be given to the user's supervisor to allow for access in a read-only mode. This information shall be treated as confidential.

e. The user must select a unique system password consisting of a combination of eight characters using characters meeting at least three of the following four criteria: lower case letter, upper case letter, number and special character (e.g., *, #, etc.).

f. Users should log out of their workstation if they must leave it unattended for more than 15 minutes.

g. Computer system access shall be disabled for employees who are expected to be gone for more than 30 calendar days. Supervisors are responsible for informing the HCA Help Desk of the employee's departure date and return date.

h. Only I.S. staff, or those authorized by I.S. staff for specific purposes, are permitted to install, modify, or remove computer hardware/software.

i. Users must not use or install personally owned software/hardware on HCA-owned or leased equipment. If a user believes that personally owned hardware/software will enhance his job performance, the user shall work with management and, if appropriate, will submit a Service Request that identifies this as an emerging hardware/software requirement to I.S.

j. Users who observe a violation of the standards within this policy are encouraged to notify their immediate supervisor and/or the HCA's Audit Manager as soon as possible.

11. **<u>Audit logs are kept of all users' Internet access.</u>**

These logs are reviewed by the Audit Manager and archived for future reference.

12. **<u>If a supervisor believes that an employee is misusing any component of the HCA's computer systems, he/she shall take action to review and rectify the possible misuse.</u>**

a. This may include contacting the Audit Manager and Human Resource Manager regarding a formal investigation.

13. **<u>Any request for the purchase or lease of IT assets or IT-related services will be submitted to the HCA Help Desk via email or telephone.</u>**

a. Equipment purchases must be made in accordance with applicable HCA and Washington State policies and regulations.

14. **<u>Remote access is authorized solely for the purpose of accessing agency work-related email and related files.</u>**

a. A user must coordinate remote access with his/her Program's Assistant Administrator and I.S.

b. Once permission is granted, the user must then coordinate with I.S. for the software needed to set up remote access.

c. I.S. normally does not provide hardware or software assistance but will offer telephonic support during regular work hours.

APPROVED
Executive Ethics Board
Date: 6/6/03

15. **Users authorized remote access shall ensure that they are running a virus-checking program with current up-to-date anti-virus signature files installed and enabled.**

    a. If the remote access connection is made via Digital Subscriber Line (DSL) or cable modem, then the user must both install and use a personal firewall program or else disconnect the DSL/cable modem link and dial-in remotely via modem.

    b. The remote user must have an updated anti-virus application enabled on his/her system prior to installing the remote access software and must continue to maintain updated anti-virus signature files.

    c. Information regarding anti-virus and personal firewall programs for home use is available from I.S.

16. **All network computer systems are backed up on a daily basis.**

    a. Users should identify critical data files on their hard drive that need to be saved in the event of a system failure.

    b. I.S. can assist in developing back-up strategies for critical hard drive and network drive files.

    c. HCA's backup strategy is designed for disaster recovery in the event of a catastrophic server failure.

    d. Oftentimes IS is able to restore files that a user has erroneously deleted; however, users should not rely on HCA's backups as their sole recovery strategy.

17. **As with all other HCA policies, failure to adhere to this policy may result in corrective or disciplinary action, up to and including dismissal.**

APPROVED
Executive Ethics Board
Date: 6/6/03